Scams

Do not open your door to anyone claiming they can test you immediately for a price. They do not have the means to test anyone and only want your money
Apple is not giving out free iPhone 11 phones with updates on the virus. If you are offered a free phone, it is most likely to get your personal information.
Cybercriminals are pretending to be from the Centers for Disease Control selling unapproved products to "combat" the virus - teas, essential oils, and colloidal silver. These products could cause serious health risks in some people. The FTC says there are no products at this time to treat or cure the virus.
Fake emails from the World Health Organization are allowing access to your personal information when you click the link. Do not open a link in an email.
There are other links to emails regarding important information on the virus. Once you click on the link, they can gain access to your personal information or download malware to corrupt your computer. It is better for you to do your own research on the internet from known news sites.
Fake fundraisers are circulating to help those affected. You can check legitimate charities through BBB Wise Giving Alliance, Charity Navigator, Charity Watch, and GuideStar. Nasconet.org is also a good place to start; it is a state regulator where charities must register for donations.
Strangers are approaching seniors, offering to shop for them and to deliver their groceries. Do not open the door to strangers and do not give strangers money. Ask friends and family for assistance first. If there is no help available from loved ones, then choose to order groceries directly from the store or reach out to resource assistance organizations such as the Aging and Disability Resource Center at Direction Home for information on available resources.
Investments in research and development scams: Seniors are receiving phone calls regarding investment opportunities in companies that are purportedly researching and developing a vaccine. Legitimate investments will not seek funding through random phone campaigns. Contact your personal licensed investment advisor or the state Attorney General's office to verify veracity.
Home sanitation scam: Seniors are being targeted with phone or online offers to have their homes cleaned and sanitized, but these offers require prepayment.
Supply scams: Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.
Provider scams: Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.

Facebook challenge scams: Trends going around on social media consist of challenges and questionaires that encourage you to post personal information. Sharing information like cars you've owned, what high school you graduated from, the year you graduated, where you were born, your mother's maiden name, etc. can all be used by hackers to bypass security questions for your online accounts.
Fake check scams: Someone sends you a check or money order and asks you to deposit it in your account and wire transfer back the money, minus a nice bonus for you, a “thank you” for helping. Regardless of the pitch, the result is the same: The check or money order you received is counterfeit. It will be returned to your bank unpaid, and the full amount will be deducted from your account.(Ohio Attorney General Dave Yost)
Grandparent scams: A con artist poses as your grandchild, claims to be in trouble, and asks you to send money via wire transfer or prepaid card. If you’re suspicious, ask a question only a family member would know how to answer, and call your son or daughter to confirm the claim. (Ohio Attorney General Dave Yost)
Home improvement scam: Door-to-door contactors offer to repair your roof, pave your driveway, or trim your trees for a great price. After you pay, the contractor disappears without doing the work or after doing a poor job. Never pay in full upfront. If you are solicited at your home, you have three days to cancel the contract, and work should not begin within that period. (Ohio Attorney General Dave Yost)
Fake Check Scams: Someone sends you a check or money order and asks you to deposit it in your account and wire transfer back the money, minus a nice bonus for you, a “thank you” for helping. Regardless of the pitch, the result is the same: The check or money order you received is counterfeit. It will be returned to your bank unpaid, and the full amount will be deducted from your account. (Ohio Attorney General Dave Yost)
Fake text message scams: texts claiming to be from governmental agencies with links to take an "online coronavirus test" or claiming that you've come into contact with someone who has tested positive for COVID-19. Please do not follow these links.
IRS Scam: The IRS will never call and ask for personal or financial information. An IRS COVID-19 Stimulus Check phone scam has been reported; the IRS will not contact you for your bank account information. https://www.irs.gov/newsroom/tax-scams-consumer-alerts. (Summit County EMA)
COVID-19 Cures: Offers for a COVID-19 vaccine, cure, or treatment via emails, online ads, or unsolicited sales. (Summit County EMA)
COVID-19 Supplies: Companies offering COVID-19 products and supplies. Check online for company validity and customer reviews. Avoid companies whose customers have complained about not receiving items. (Summit County EMA)
Hoarding and Price Gauging PPE and essential supplies: To report, please visit https://justice.gov/coronavirus.(Summit County EMA)
VPN Cyber Threat: Cyber attackers are likely to target VPN vulnerabilities as more people telework due to COVID-19.(Summit County EMA)

Falsified Medical Documents: FBI warns of individuals providing falsified medical documents claiming positive COVID-19 test results to employers.(Summit County EMA)
“County” utility calls: Calls received from spoofed 643 numbers related to utility payments. These calls are not actually Summit County numbers and should be ignored; do not respond to voicemails. (Summit County EMA)
Dominion Energy: Scammers are going door to door posing as Dominion Energy representatives and threatening to disconnect service unless payment is collected. The utility will never call, text or email customers to request personal information such as their Social Security numbers, credit card numbers, or bank account numbers. All company employees carry a photo ID card. Residents can call Dominion Energy at 800-362-7557 to report a suspected scam. (Summit County EMA)
Robocalls offering respiratory masks they won't ever send
Social media posts: fraudulently seeking donations for non-existent charities, or claiming to give you stimulus funds if you enter your bank account information
Fake testing kits, cures, "immunity" pills, and offers for protective equipment
Imposter scam- says they are a government official (IRS, Office of President, your unspecified "bank"), saying they need information to process stimulus check (should arrive automatically) or need updated personal information in case of emergency (unlikely)
Grandparent scam- a "grandchild" pretending to lose his/her job due to COVID-19, asking for a wire transfer and not to tell parents
Sweetheart scam- new "love interest" learns of stimulus check arrival, says they lost job to COVID-19 and need your check money
Refinance/Mortgage scam- homeowner trying to refinance loan or get mortgage help due to OCVID-19 struggles, do not give information to a company/agent that is not your current lender (if it is valid they should be able to direct you to your company or individual. You can also reach out to them directly first)

Advice from the US Attorney's Office Regarding Scams

Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.
Check the websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use “cdc.com” or “cdc.org” instead of “cdc.gov.”
Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the general public this way.
Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.
Make sure the anti-malware and anti-virus software on your computer is operating and up to date.
Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if there is a medical breakthrough, you won’t hear about it for the first time through an email, online ad, or unsolicited sales pitch.
Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving. Remember, an organization may not be legitimate even if it uses words like “CDC” or “government” in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.
Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Don’t send money through any of these channels.
Be cautious of “investment opportunities” tied to COVID-19, especially those based on claims that a small company’s products or services can help stop the virus. If you decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website.
For the most up-to-date information on COVID-19, visit the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) websites.